Renmaker

Independent Cleantech Consultancy

Solar & Battery Security Checklist

How to Safely Isolate High-Risk Components

Version 1.0 — July 2026

Renmaker Ltd.

Prepared by: John Mustardé

Solar & Battery Security Checklist

1. Network Isolation

- Place all inverters, BESS units, dataloggers and gateways on a **dedicated VLAN or physically separate subnet**.
- Ensure **no direct route** to corporate IT systems.
- Ensure **no direct route** to the open internet.
- Disable Wi-Fi unless explicitly required and secured.
- Document the network diagram and store it with system O&M files.

2. Install a Secure, EU-Vetted Gateway

A hardware gateway must sit between the device and the internet.

The gateway must:

- Intercept all outbound traffic
- Block unauthorised destinations
- Filter telemetry
- Enforce data localisation
- Log every packet
- Control and audit remote access
- Terminate all external connections at the gateway (never at the inverter)

Record:

- Gateway model
- Firmware version
- Configuration file
- Change-control log

3. Outbound Traffic Whitelisting

Block everything by default.

Only allow:

- One EU endpoint
- One port
- One protocol
- One defined frequency

If the device attempts any other connection → **drop it**.

Document:

- Allowed IPs
- Allowed ports
- Allowed protocols
- Monitoring rules

4. Remote Access Control

All remote access must:

- Terminate at your gateway
- Use multi-factor authentication
- Be time-limited
- Be manually approved
- Be fully logged

Never allow:

- Vendor VPN
- Vendor SSH
- Direct cloud override
- Unsupervised remote commands

Record:

- Remote access policy
- Access logs
- Approval workflow
- Vendor access agreements

5. Block Automatic Firmware Updates

- Disable OTA updates
- Block remote reboot commands
- Only allow manually approved updates
- Validate firmware before installation
- Test updates offline before deployment

Document:

- Firmware version history
- Update approval records
- Offline test results
- Vendor release notes

6. Local Telemetry Mirroring

- Store all operational data locally
- Compare local vs cloud telemetry
- Detect anomalies or manipulation
- Maintain operational continuity if cloud services fail

Record:

- Local storage location
- Retention policy
- Comparison logs
- Anomaly detection rules

7. Segregate Control vs Analytics

- Control functions (dispatch, export limits, charge/discharge) must be **local**
- Analytics dashboards must be **read-only**
- Prevent cloud platforms from sending control signals

Document:

- Control system architecture
- Analytics system permissions
- Segregation policy
- Access rights matrix

8. Vendor Transparency Requirements

Your EPC/vendor must provide:

- Firmware governance documentation
- Data flow diagrams
- Cloud ownership disclosures
- Remote access policies
- Cybersecurity certifications
- Confirmation of MSP compliance under the UK Cyber Security & Resilience Bill

Record:

- Vendor declarations
- Supporting documents
- Compliance evidence
- Risk assessment notes

9. MSP Compliance Check

Your vendor is legally a Managed Service Provider (MSP) if they:

- Monitor your system
- Push firmware
- Provide remote support
- Send load-control signals
- Operate an EMS platform

Require:

- Evidence of compliance
- Incident reporting processes
- Risk management documentation
- Security controls for remote access

Document:

- MSP compliance checklist
- Incident reporting contacts
- SLA terms
- Security audit results

10. Red-Flag Conditions — When to Avoid the Vendor

Avoid the device if:

- It cannot operate without cloud connectivity
- It requires foreign cloud servers for core functionality
- It cannot be isolated without breaking operation
- The vendor refuses to disclose cloud ownership or data flows
- Firmware updates cannot be controlled locally

If any of these apply, isolation is impossible — choose a different supplier.

Record:

- Red-flag findings
- Final procurement decision
- Risk justification
- Approval sign-off